UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,753	11/21/2003	Alexander Hoffmann	16274.171	1445

22913 7590 11/20/2009

Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
11/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/718,753	HOFFMANN, ALEXANDER	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 07/31/2009.

2. Claims 1-36 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1, 13, 22, 25, 29 and 32 have been considered but are moot in view of the new ground(s) of rejection.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claim 3 recites "the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver", which is not described in the specification.

Claim 25 recites "authenticating the fiber optic transceiver independent of the received data signals", which is not described in the specification.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 25-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 25-28 use the phrase "means for", but it is modified by some structure, material, or acts recited in the claim. It is unclear whether the recited structure, material, or acts are sufficient for performing the claimed function which would preclude application of 35 U.S.C. 112, sixth paragraph, because the specification does not provide any specific structure closely associated to the recited functions in these claims. For instance, there are no descriptions in the disclosure for means that is used for authenticating the fiber optic transceiver independent of the received data signals upon installation of the fiber optic transceiver. One skilled in the art cannot know what structure is meant for "means for" since no algorithms for performing the functions are described.

A general allegation that these are simple programs that one skilled in the art can make is not sufficed. In order to meet the requirements for a claim in "means plus function" format the relevant algorithms should be disclosed in the specification. If applicant wishes to have the claim limitation treated under 35 U.S.C. 112, sixth paragraph, applicant is required to amend the claim so that the phrase "means for" or "step for" is clearly **not** modified by sufficient structure, material, or acts for performing the claimed function.

If applicant does **not** wish to have the claim limitation treated under 35 U.S.C. 112, sixth paragraph, applicant is required to amend the claim so that it will clearly not

be a means (or step) plus function limitation (*e.g.*, deleting the phrase "means for" or "step for").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al (US 2003/0108199 A1), hereinafter Pinder, in view of the applicant admitted prior knowledge described in the background section of the specification and hereinafter referred to as APK.

Pinder discloses a system with a digital subscriber communication terminal (DSCT) (see Fig. 1, 110) to receive, decode and process the incoming signals to be displayed on the subscriber's display unit (see, e.g., [0040]). The DSCT provides a two-way interface between a digital broadband delivery system (DBDS) and the subscriber (see Fig. 1, DSCT 110 and DBDS 100). The DSCT is equipped with a transceiver, which is used by the DSCT to have two-way communication with the sender of the signal programming to the subscriber location (see, e.g., [0102] and [0109]). Thus, when it is referred to the authentication of the DSCT it also means authentication of the

transceiver, because the transceiver is an integral part of the DSCT and provided by the manufacturer.

Regarding claims 1 and 13, Pinder discloses:

a host (see, e.g., Fig. 1, headend 102 or the block 106 correspond to the host);

an interface electrically coupled to the host (see, e.g., [0040]); and

a transceiver comprising:

a transmitter configured to transmit data signals (see, e.g., [0072], where "receive messages from the DSCT 110" indicates that the transceiver equipped with a transmitter);

a receiver configured to receive data signals (see, e.g., [0106], where "transmitted to the DSCT 110" indicates that the transceiver equipped with a receiver); and

a controller configured to encrypt a string and supply the encrypted string to a host to authenticate the transceiver (see, e.g., [0066], where a message is signed by the DSCT 110 which is the same as the transceiver and sent to the TED 302 located at the headend which is considered to be the host),

authentication of the transceiver being contingent upon whether or not the transceiver has been certified by a manufacturer of the transceiver or a supplier of the transceiver (see [0057], where the manufacturer provides the public key and the serial number of the DSCT 110 to the control system of the headend which corresponds to the recited host and the control system verifies the authenticity of the DSCT 110 certificate provided by the manufacturer; [0066], where the public key of the DSCT linked to its serial number, is

retrieved from the control system database by the CPU 304 of the control system located at the headend for authentication of the DSCT which also means the authentication of the transceiver. This process indicates that the authentication of the DSCT or the transceiver depends on the authenticity of the transceiver or its certification by the manufacturer).

Pinder, however, does not expressly disclose that the transceiver is certified by the manufacturer to meet a specified quality standard which means that the transceiver is not a cloned one. APK discloses that the transceiver must meet strict quality standards before its deployment (see paragraph [0003] of the publication application of the instant invention).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to deploy a transceiver that meets its manufacturer's specified quality standards as described in APK in the system of Pinder in order to have a reliable transceiver instead of a cloned one to prevent possible loss due to the failure of transceiver (see APK, page 1, lines 20-28 of the specification of the instant application).

Regarding claim 22, this claim is rejected as applied to the like elements of claims 1 and 13 and further Pinder discloses:

wherein the controller stores a first unique transceiver-specific public key/private key pair for authentication, the first unique transceiver-specific public key/private key corresponding with a manufacturer of the transceiver. See [0057].

Regarding claim 25, this claim is rejected as applied to the like elements of claims 1 and 13 and further Pinder discloses:

authenticating the fiber optic transceiver independent of the received data signals upon installation of the fiber optic transceiver. See [0057], where the control system 232 verifies (i.e., authenticates) the certificate to be authentic before placing it into the database of DSCTs 110 (i.e., at the time of the installation before any communication transmitted by the transceiver).

Regarding claim 29, this claim is rejected as applied to the like elements of claims 1 and 13 and further Pinder discloses:

accepting or rejecting the transceiver by the host (i.e., whether the transceiver authenticated or not). See [0057], where the control system 232 verifies the certificate to be authentic which would result in whether to accept or reject the transceiver as authentic.

Regarding claim 2, Pinder discloses:

The transceiver of claim 1, wherein the controller is configured to encrypt the string with a transceiver private encryption key (see, e.g., [0066]; where using the public key of the DSCT 110 to authenticate that the message is in fact come from the DSCT 110 implies that the message is encrypted by the private key of the DSCT 110 or the transceiver).

Regarding claims 3 and 28, Pinder discloses:

The transceiver of claim 1, wherein the controller is configured to use a transceiver private encryption key and a transceiver public encryption key to authenticate the transceiver (examiner assumes that the recited limitation in these claims means that the controller authenticating the transceiver with the host as described in [0039] of the application publication). See, e.g., [0066], where for the authentication of the DSCT 110, its public key and private key are used.

Regarding claim 4, this claim is rejected as applied to the rejection of claim 2.

Regarding claims 5 and 6, Pinder discloses:
These claims are interpreted as described in [0039] of the application publication. wherein the transceiver public encryption key is sealed by encrypting the transceiver public encryption key with a system (examiner assumes that system is the manufacturer as described in [0039] of the application publication) private encryption key and stored as a sealed transceiver public encryption key, wherein the sealed transceiver public encryption key is decrypted with a system public encryption key to retrieve the transceiver public encryption key (see [0057], where the manufacturer provides a copy of the public key of the DSCT 110 to the control system and the control system verifies the authenticity of the DSCT 110 certificate which implies that for the purpose of the verification the public key of the DSCT 110 is encrypted by the private key of the manufacturer and decrypted by the control system applying the public key of the manufacturer as normally done in the art).

Regarding claim 7, Pinder discloses:

The transceiver of claim 1, wherein the controller comprises an electrically erasable and programmable read only memory that is used to store a transceiver private encryption key and a transceiver public encryption key (see, e.g., Fig. 6, 626).

Regarding claim 8, Pinder discloses:

The transceiver of claim 1, wherein the controller comprises a cryptography module for encrypting the string (see, e.g., [0066], where the encryption of the content indicates that the transceiver includes a cryptography module).

Regarding claim 9, Pinder discloses:

The transceiver of claim 1, wherein the controller comprises an RSA encryption module for encrypting the string (see, e.g., [0041]).

Regarding claim 10, Pinder discloses:

The transceiver of claim 1, wherein the receiver comprises a fiber optic receiver (see, e.g., [0038]).

Regarding claim 11, Pinder discloses:

The transceiver of claim 1, wherein the transmitter comprises a fiber optic transmitter (see, e.g., [0038]).

Regarding claim 12, Pinder discloses:

The transceiver of claim 1, wherein the transceiver comprises a small form factor pluggable transceiver (see, e.g., Fig. 1, DSCT 110 is an indication of a small form factor; see also [0035], where a telephone is normally is of small size and its transceiver consequently is small form factor).

Regarding claim 14, Pinder discloses:

The network system of claim 13, wherein the interface comprises an inter-integrated circuit bus (see, e.g., Fig. 6, where the bus 620 is integrated in the DSCT for communication purpose).

Regarding claim 15, Pinder discloses:

The network system of claim 13, wherein the interface comprises a transceiver fault status line (see, e.g., [0127], where a verification failure indicates that the system of Pinder has a mechanism for ending the communication which corresponds to the recited transceiver fault status line or disable line).

Regarding claim 16, the same rationale applied to claim 15 is applicable here.

Regarding claim 17, Pinder discloses:

The network system of claim 13, wherein the interface comprises a transmit data in line TD+ and an inverted transmit data in line TD- (see, e.g., Fig. 6, where the transmission and receiving lines 154 and 256 for communication are shown).

Regarding claim 18, Pinder discloses:

The network system of claim 13, wherein the interface comprises a received data out line and an inverted received data out line (see, e.g., Fig. 6, where the transmission and receiving lines for communication are shown).

Regarding claim 19, Pinder does not expressly disclose:

The network system of claim 13, wherein the interface comprises a loss of signal status line.

The examiner, however, takes official notice that the deployment of a loss of signal status line is well known in the art. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to deploy a loss of signal status line in the system of Pinder in order to indicate to the subscriber the strength of the incoming signals or the continuation or discontinuation of the incoming signals.

Regarding claim 20, Pinder discloses:

The network system of claim 13, wherein the host is one of a mainframe computer, a workstation, a server, and a storage device (see, e.g., [0050], Fug. 2).

Regarding claim 21, Pinder discloses:

The network system of claim 13, wherein the host is one of a bridge, a router, a hub, a local area switch and a wide area switch (see, e.g., [0039]; [0051]; Fig. 1, 104).

Regarding claims 26 and 27, Pinder discloses:

The fiber optic transceiver of claim 25, wherein the means for receiving data signals comprises means for converting optical serial data into electrical serial and the means for transmitting data signals comprises means that does the reverse operation (see [0047]; [0047]-[0048], where a modulator is used to convert the signals suitable for transmission).

Regarding claim 30, Pinder discloses:

The method of claim 29, wherein the authentication signal comprises a certificate identification (see, e.g., [0066], where the DSCT 110 public key corresponds to the recited certificate identification).

Regarding claim 31, Pinder discloses:

The method of claim 29, wherein analyzing the authentication signal comprises decrypting the authentication signal using a public key of an issuing authority (see, e.g., [0057], where the verification of the certificate by the control system corresponds to the recited analyzing the authentication signal).

Regarding claim 32, this calim is rejected as applied to claims 1, 13, 22, 25 and 29 above and Pinder further discloses:

A method for authenticating a transceiver, comprising:

installing a transceiver comprising a transceiver specific public key/private key pair, wherein the transceiver specific public key is encrypted with a private key of an issuing authority (see, e.g., [0057] and [0068]).

electrically coupling the transceiver to a host through a communication link (see, e.g., Figs. 1, where DSCT 110 is coupled to headend 102 or Hub 104 through communication link 154);

requesting, by the host, the encrypted transceiver specific public key from the transceiver (see, e.g., [0057], where providing the public key of the DSCT 110 to the control system of the headend corresponds to the requesting…);

passing the encrypted transceiver specific public key from the transceiver to the host by way of the communication link (see, e.g., Fig. 1, where link 154 is used for communication between the DSCT 110 and the headend); and

decrypting the encrypted transceiver specific public key in the host using a corresponding public key of the issuing authority to obtain the transceiver specific public key (see [0066] and the rationale applied to the claims 5 and 6 above).

Regarding claim 33, Pinder discloses the use of the public key of the DSCT (i.e., transceiver) for authentication of the DSCT by the headend, but does not clearly describe the limitations recited in this claim (see [0057] and [0066]). However, the

examiner takes official notice that the limitations recited in this claim are a common authenticating procedure that is widely used in the cryptographic technology. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to incorporate the well known scheme recited in this claim in the system of Pinder for the purpose of authenticating the transceiver with the headend (i.e., host).

Regarding claim 34, this claim is rejected as applied to the like elements of claim 29 and further Pinder discloses:
comparing the decrypted authentication string to the original authentication string (see [0066]).

Regarding claim 35, Pinder discloses:
The method of claim 33, wherein the original authentication string is a random number (see, e.g., [0092]).

Regarding claim 36, this claim is rejected as applied to the like elements of claims 1 and 13 above.

Regarding claims 23 and 24, Pinder discloses:
A unique serial number or IP address (corresponding to the recited access code) is assigned to each transceiver (see [0057]) that is transmitted to the control system of the

headend (i.e., host) along with the public encryption key of DSCT for the purpose of DSCT (i.e., transceiver) certificate authentication. Since the unique serial number is used with the public encryption key for the same purpose and belong to the same transceiver, thus unique serial number is associated with the public encryption key. With respect to a second access code associated with a second public/private key pair, Official Notice is taken that in order to have a strong security system, it is old and well known practice in the art of cryptography to have other cryptographic keys for replacement and substitution of the keys that are currently used either when the keys are expired or if it is suspected that the keys have been used by an unauthorized entity. Therefore, the teachings of Pinder meet the limitations of claims 23 and 24, i.e., the following:

wherein the first unique transceiver-specific public key/private key pair is associated with a first access code and the controller stores a second unique transceiver-specific public key/private key pair for authentication, wherein the second unique transceiver-specific public key/private key pair is associated with a second access code.

wherein the first unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the first access code to the controller and the second unique transceiver-specific public key/private key pair is used for authentication in response to the host communicating the second access code to the controller.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. N./
Abdulhakim Nobahar
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432